Homeland Security

Federal Bureau of Investigation

JOINT INDICATOR BULLETIN

Distributed as TLP: GREEN

Reference Number: JIB-14-20199C

Destructive Malware

12 February 2015

UPDATE to JIB-14-20199B *(released 15 December 2014):* DHS and FBI will continue to update this document as more information becomes available. ***(Note: Text preceded with an asterisk and italicized indicates new or updated information).***

Summary

This Joint Indicator Bulletin (JIB)[1] is the result of efforts between the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT) and the Federal Bureau of Investigation (FBI) to highlight known cyber threat indicators.

The US-CERT and the FBI are providing the following information with **HIGH** confidence**:** Destructive malware was used, and may currently be in use, by unknown computer network exploitation (CNE) actors. This malware has the capacity to overwrite a victim host's master boot record (MBR) and all data files. Subsequent attempts to recover data using standard forensic methods will be difficult, costly, and potentially impossible.

[1] *A JIB is intended to provide indicators derived from new cyber incidents and/or malicious code that can pose a threat to federal, state, local, tribal, and territorial government, critical infrastructure, private industry, or international partners.*

Background

In late November 2014, employees of a U.S. business experienced defacement on their computer desktops when employees logged in to their workstations. The defacement indicated that the malicious activity would continue and the U.S. business' data would be released publically. Later that day, the malware propagated through the company's global network, and the network was ultimately taken offline.

Technical Data

Analysis

US-CERT and the FBI are providing the following information with **HIGH** confidence**:**

This group uses some custom tools that should be flagged immediately upon detection, reported to the FBI, and given highest mitigation priority. The aforementioned actors have used identified domain names and IP addresses as source and/or destination IP addresses. The FBI is distributing the indicators associated with a successful attack to enable network defense activities and reduce the risk of similar attacks in the future. The FBI has high confidence that these indicators are being used by CNE actors for further network exploitation. The FBI recommends that your organization help victims identify and remove the malicious code. Below are descriptions of malware and associated signatures:

The malware was designed to propagate throughout the network via Windows file shares which are often enabled by default, if not enabled, the malware has the ability to turn on remote sharing of the windows system directory and begin wiping process. After each successful deployment of the wiper to a remote file-system, the malware reports its status back to several command and control (C2) IP addresses. The wiper component contained three different methods for erasing files on the remote host's physical drive accessed via a device driver, local wiping of files by searching for files on disk, and remote wiping of files via the network share. The two dropped files which did not contain wipers or configuration files may have been used for testing of the implant.

A summary of the C2 IP addresses from the analyzed files is provided in the table on the next page.

Table 1: Summary of C2 IP Addresses			
IP Address	**Country**	**Port**	**Filename**
203.131.222.102	Thailand	8080	Diskpartmg16.exe igfxtrayex.exe igfxtpers.exe
217.96.33.164	Poland	8000	Diskpartmg16.exe igfxtrayex.exe
88.53.215.64	Italy	8000	Diskpartmg16.exe igfxtrayex.exe
200.87.126.116	Bolivia	8000	--
58.185.154.99	Singapore	8080	--
212.31.102.100	Cypress	8080	--
208.105.226.235	United States	--	igfxtpers.exe
** 116.255.139.223*	*China*	*443*	--

File Information:

Name: d1c27ee7ce18675974edf42d4eea25c6.bin
Size: 268579 bytes (268.6 KB)
MD5: D1C27EE7CE18675974EDF42D4EEA25C6
PE Compile Time (UTC): 2014-11-22 00:06:54
Language pack of resource section: Korean
** Import Hash: 8B64D3EA6711C7E0A4E57BD12B350E2E*

The malware has the following characteristics:

** When executed, the file installs itself as a service and drops "igfxtrayex.exe."* It then attempts to connect back to the command and control IPs to report control code "0x28" and the hostname of the system. Additionally, when "diskpartmg16.exe" was executed, it started a second instance of itself with "-i" as an argument, and then terminated. The second instance of the dropper file installed itself as the "WinsSchMgmt" service with "-k" as a command line argument, started the service, and then terminated. The "WinsSchMgmt" service executed the file with "-k" as an argument, which started another instance of the file using "-s" as an argument. The "-s" instance dropped and executed "igfxtrayex.exe", created "net_ver.dat", and began generating network traffic over TCP ports 445 and 139 to victim IP addresses. The following files were added:

C:\Documents and Settings\User\Desktop\igfxtrayex.exe
C:\WINDOWS\system32\net_ver.dat

See Appendix A for strings of interest associated with this dropper file.

File Information:

Name: net_ver.dat
Size: 4572 bytes (4.6 KB) (size will vary)
MD5: 93BC819011B2B3DA8487F964F29EB934 (hash will vary)

This is a log file created by the dropper, and appended to as the scans progress It contains what appear to be hostnames, IP addresses, and the number 2. Entries in the file have the structure "HOSTNAME | IP Address | 2".

File Information:

Name: igfxtrayex.exe
Size: 249856 bytes (249.9 KB)
MD5: 760C35A80D758F032D02CF4DB12D3E55
PE Compile Time (UTC): 2014-11-24 04:11:08
Language pack of resource section: Korean
** Import Hash: BCFDBEEC0DD613A17BD97CB8D9446949*

This file is destructive malware: a disk wiper with network beacon capabilities. If "igfxtrayex.exe" is run with no parameters, it creates and starts a copy of itself with the "–i" argument. After 10 minutes, the "igfxtrayex.exe" makes three copies of itself and places them in the same directory from which it was executed. These copies are named according to the format "taskhostXX.exe" (where X is a randomly generated ASCII character). These copies are then executed, each with a different argument (one being "-m", one being "-d" and the other "-w"). Network connection attempts are made to one of three hard-coded IP addresses in a random order to port 8080 or 8000. If a connection to the IP address cannot be made, it attempts to connect to another of the three IP addresses, until connections to all three IP addresses have been attempted. The following command-line string is then executed: "cmd.exe /c net stop MSExchangeIS /y". A 120-minute (2 hour) sleep command is issued after which the computer is shut down and rebooted.

** Additionally, "igfxtrayex.exe" drops "taskhostXX.exe", "iissvr.exe", "usbdrv3.sys", and a second file name of "usbdrv3.sys". During dynamic analysis it created the files: "taskhostcs.exe", "taskhostdg.exe", and "taskhosthr.exe".*

File Information:

Name: iissvr.exe
Size: 114688 bytes (114.7 KB)
MD5: E1864A55D5CCB76AF4BF7A0AE16279BA
PE Compile Time (UTC): 2014-11-13 02:05:35
Language pack of resource section: Korean
** Import Hash: A97BACFCF82310A4634B40947B919DA*

This file, when executed, starts a listener on localhost port 80 and displays the webpage defacement. It has 3 files contained in the resource section; all xor'd with 0x63. The webpage points to several additional websites which allegedly contain proof of the hack. These websites have also been noted in open source reporting of the intrusion.

File Information:

Name: usbdrv3_32bit.sys
Size: 24280 bytes (24.3 KB)
MD5: 6AEAC618E29980B69721158044C2E544
PE Compile Time (UTC): 2009-08-21 06:05:32

This SYS file is a commercially available tool that allows read/write access to files and raw disk sectors for user mode applications in Windows 2000, XP, 2003, Vista, 2008 (32-bit). It is dropped from resource ID 0x81 of "igfxtrayex.exe". It is signed with a valid digital signature with a timestamp of Friday, August 21, 2009 at 1:05:48 am.

File Information:

Name: usbdrv3_64bit.sys
Size: 28120 bytes (28.1 KB)
MD5: 86E212B7FC20FC406C692400294073FF
PE Compile Time (UTC): 2009-08-21 06:05:35

This SYS file is a also a commercially available tool that allows read/write access to files and raw disk sectors for user mode applications in Windows 2000, XP, 2003, Vista, 2008 (64-bit). It is dropped from resource ID 0x83 of "igfxtrayex.exe".

File Information:

Name: igfxtpers.exe
Size: 91888 bytes (91.9 KB)
MD5: E904BF93403C0FB08B9683A9E858C73E
PE Compile Time (UTC): 2014-07-07 08:01:09

****File Information:***

Name: 57BEB768CC3E42A96A1725A5E9959A54
Size: 430755 bytes (430.8 KB)
MD5: 57BEB768CC3E42A96A1725A5E9959A54
PE Compile Time (UTC): 2014-11-22 04:05:02
Import Hash: F75154B82A26247B6569415188F114DB

This file contains the same code as "diskpartmg16.exe", but this file is not dropped. This file also contains the network communication components, but it lists different C2 IP address than the previous files. These IP Addresses include: 200.87.126.116, 58.185.154.99, and 212.31.102.100. Because the file is lacking an embedded config file, the network communication between the target and C2 is not established.

**** File Information:***

Name: 87A1D976E37A525026C819491D7B62B2
Size: 430709 bytes (430.7 KB)
MD5: 87A1D976E37A525026C819491D7B62B2
PE Compile Time (UTC): 2014-11-22 04:05:02
Import Hash: F75154B82A26247B6569415188F114DB

This file is nearly identical to the previous file, "57BEB768CC3E42A96A1725A5E9959A54". However, this file is 48 bytes less than the previous file. The last 48 bytes are zeroes.

Network Propagation Wiper

The malware has the ability to propagate throughout the target network via built-in Windows shares. Based on the username/password provided in the configuration file and the hostname/IP address of target systems, the malware will access remote network shares in order to upload a copy of the wiper and begin the wiping process on these remote systems. The malware uses several methods to access shares on the remote systems to begin wiping files. Checking for existing shares via "\\hostname\admin$\system32" and "\\hostname\shared$\system32" or create a new share "cmd.exe /q /c net share shared$=%SystemRoot% /GRANT:everyone, FULL". Once successful, the malware uploads a copy of the wiper file "taskhostXX.exe", changes the file-time to match that of the built-in file "calc.exe", and starts the remote process. The remote process is started via the command "cmd.exe /c wmic.exe /node:hostname /user:username /password:pass PROCESS CALL CREATE". Hostname, username, and password are then obtained from the configuration file. Afterwards, the remote network share is removed via "cmd.exe /q /c net share shared$ /delete". Once the wiper has been uploaded, the malware reports its status back to one of the four C2 IP addresses.

Feedback

We strive to make the JIB a valuable tool for our partners, and welcome feedback on how this publication could be improved. You can help by answering a very short series of questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.

Points of Contact

Recipients of this bulletin are encouraged to contribute additional information related to this cyber threat malicious activity leveraging social media sites, or other similar activity. Include the

JIB reference number in the subject line of all email correspondence. For any questions related to this report, please contact NCCIC/US-CERT or the FBI at:

NCCIC/US-CERT:
(UNCLASS) Phone: +1-703-235-8832
(UNCLASS) Email: soc@us-cert.gov
(SIPRNET) Email: us-cert@dhs.sgov.gov
(JWICS) Email: us-cert@dhs.ic.gov

FBI:
(UNCLASS) Phone: +1-855-292-3937
(UNCLASS) Email: cywatch@ic.fbi.gov
(SIPR)Email: cywatch@fbi.sgov.gov
(JWICS) Email: cywatch@fbi.ic.gov

Appendix A

Table 2 identifies the strings associated with the file information below:

Name: d1c27ee7ce18675974edf42d4eea25c6.bin
Size: 268579 bytes (268.6 KB)
MD5: D1C27EE7CE18675974EDF42D4EEA25C6
PE Compile Time: 2014-11-22 00:06:54
Language pack of resource section: Korean

Table 2: Malware string correlating to filename: d1c27ee7ce18675974edf42d4eea25c6.bin

- - - BEGIN STRINGS - - -
recdiscm32.exe
taskhosts64.exe
taskchg16.exe
rdpshellex32.exe
mobsynclm64.exe
comon32.exe
diskpartmg16.exe
dpnsvr16.exe
expandmn32.exe
hwrcompsvc64.exe
cmd.exe /q /c net share shared$ /delete
\\%\admin$\syswow64
\\%s\admin$\system32
cmd.exe /q /c net share shared$=%SystemRoot%
cmd.exe /q /c net share shared$=%SystemRoot% /GRANT:everyone, FULL
RasSecruity
RasMgrp

cmd.exe /c wmic.exe /node: ”%s” /password: “%s” PROCESS CALL CREATE “%s” >

%s
WinsSchMgmt
Windows Schedule Management Service

- - -END STRINGS - - -

Analyst Comment:
When the dropper is executed, it scans the local network using a predetermined list of hostnames and IP addresses. Scan traffic is designed to appear as NETBIOS & Microsoft-DS traffic over 139 & 445. The malware attempts to propagate by mapping the default hidden shares ADMIN$ & IPC$ of any system that responds with an ACK, using a known set of domain accounts hard-coded in the malware. If successful, the malware will have full control over the remotely mapped host and will copy the original dropper to the “windows\System32” folder, renamed as “comon32.exe”.The file “comon32.exe” is executed, “igfxtrayex.exe” is dropped, and the process begins again.

Appendix B

FBI developed the Snort and YARA signatures included below that can be implemented to detect the aforementioned malicious traffic.

UPDATE: Due to the rapidly evolving course of inquiry into this malware, information obtained has been provided as soon as it develops. The following Snort signature was previously provided in an early version of this message; recently obtained information indicates that this signature may be inaccurate.

Figure 1: FBI-developed Snort Signature

Alert tcp any any - > [88.53.215.64, 217.96.33.164, 203.131.222.102] [8080, 8000] (msg: "wiper_callout"; dsize:42; content: "|ff ff ff ff|"; offset: 26; depth: 4; sid: 314;)

Despite this new information, however, we cannot definitively discount the above signature as having value for identification of malicious traffic. Although, this information does indicate that the following two new Snort rules may also be of value:

alert tcp any any -> any [8000,8080] (msg:"WIPER_STARTED_MSG"; flow: established, to_server; dsize:42; content:"|28 00|"; depth:2; content:"|04 00 00 00|"; offset:38; depth:4; sid:123;)

alert tcp any any -> any [8000,8080] (msg:"SPREAD_SUCCESS_MSG"; flow: established, to_server; dsize:42; content:"|28 00|"; depth:2; content:"|01 00 00 00|"; offset:38; depth:4; sid:124;)

In addition to the Snort signature outlined on Figure 1, the NCCIC/US-CERT recommends searching for outbound network traffic over TCP port 445 (SMB) traffic as this would be indicative of possible suspicious activity.

Figure 2: FBI-developed YARA Signature

```
rule unknown_wiper_str{

meta: unique string in wiper malware

strings:
$STR1 =
"#99E2428CCA4309C68AAF8C616EF3306582A64513E55C786A864BC83DAFE0C78585B6
92047273B0E55275102C66" fullword nocase
$MZ = "MZ"

Condition:
$MZ at 0 and $STR1
```

```
}
rule unknown_wiper_IPs{

meta: unique IPs in wiper malware

strings:
$IP1 = "203.131.222.102" fullword nocase
$IP2 = "217.96.33.164" fullword nocase
$IP3 = "88.53.215.64" fullword nocase
$MZ = "MZ"

condition:

$MZ at 0 and all of them

}

rule unknown_wiper_error_strings{

meta: unique custom error debug strings discovered in the wiper malware

strings:
$ERR1 = "$MFT Record read failed." fullword nocase
$ERR2 = "Drive Boot Sector read failed." fullword nocase
$ERR3 = "SetFilePointer failed." fullword nocase
$MZ = "MZ"

condition:
        $MZ at 0 and all of them
}
```

Appendix C

Table 3 identifies antivirus (AV) vendors that detect this malware:

Table 3: AV Vendors Correlating to the destructive malware	
Company	**Malware Name**
ALYac	Backdoor.Destover.A
AVG	Generic36.ALDA
AVware	Trojan.Win32.Generic!BT
Ad-Aware	Trojan.NukeSped.A
BitDefender	Trojan.NukeSped.A
ClamAV	Win.Trojan.NukeSped
Cyren	W32/Wiper.MRHI-3910
DrWeb	Trojan.DownLoader11.49004
F-Prot	W32/Wiper.A
F-Secure	Trojan.NukeSped.A
Fortinet	W32/Wiper.SNAT!tr
GData	Trojan.NukeSped.A
Ikarus	Trojan-Spy.Netver
Kaspersky	Trojan.Win32.Destover.a Trojan.Win32.Destover.d
Malwarebytes	Trojan.NukeSped.SMW
McAfee	Trojan-Wiper Trojan-FFJQ!E904BF93403C
McAfee-GW-Edition	BehavesLike.Win32.PWSTravNet.dc
MicroWorld-eScan	Trojan.NukeSped.A
Microsoft	Trojan:Win32/NukeSped.A!dha Backdoor:Win32/Escad.A
Qihoo-360	HEUR/QVM07.1.Malware.Gen
Sophos	Troj/Destover-C
Symantec	Backdoor.Destover
TrendMicro	BKDR_WIPALL.A
TrendMicro-HouseCall	BKDR_WIPALL.A
VIPRE	Trojan.Win32.Generic!BT
ViRobot	Dropper.Agent.268579